TAMPEREEN TEKNILLINEN YLIOPISTO
TAMPERE UNIVERSITY OF TECHNOLOGY

MARKO LEHTONEN

DATAN MANIPULOINTI KYBERHYÖKKÄYKSESSÄ

Kandidaatintyö

Tarkastaja: Yliopisto-opettaja Marko Helenius
Tarkastaja ja aihe hyväksytty
Tieto- ja sähkötekniikan tiedekunta-neuvoston kokouksessa 7.9 2016

TIIVISTELMÄ

Marko Lehtonen: Datan manipulointi kyberhyökkäyksessä
Tampereen teknillinen yliopisto
Kandidaatin työ, 25 sivua
Lokakuu 2017
Tietotekniikan kandidaatin tutkinto-ohjelma
Pääaine: Ohjelmistotuotanto
Tarkastaja: Yliopisto-opettaja Marko Helenius

Avainsanat: kyber, data, hyökkäys, manipulointi

Kyberhyökkäyksiä on tapahtunut tietoverkoissa jo pitkään. Yleisimmin kohteen kone on joko lukittu tai sieltä on varastettu dataa. Uusi uhka datalle on, että sitä muokataan alkuperäisestä. Tällä tavoin voidaan saada kriittiset järjestelmät toimimaan väärin tai jopa rikkoa ne. Vaikka tällaisia hyökkäyksiä ei ole vielä dokumentoitu, ainakaan julkisesti, koetaan niiden uhan kasvavan.

Tämän työn tavoitteena on selvittää, millainen uhka datan manipulointi on ja mitä data manipulointihyökkäyksellä voidaan saavuttaa. Työssä tarkastellaan myös mahdollisien hyökkääjien profiileja ja kohteita. Tietoja hyökkäyksistä ja uhasta saatiin paljolti kyberturvallisuusjulkaisuista ja -tutkimuksista. Tietoja käytetään työssä uhkakuvien todentamiseen ja hyökkäyksen vaikutuksien arviointiin.

Tutkimus osoitti, että datamanipulaation uhka on todellinen. Hyökkäys vaatii tosin hyökkääjältä runsaasti resursseja, jotta hyökkäyksestä saadaan hyötyä. Samalla tosin havaittiin, että hyökkäyksen suorittaminen vaatii aikaa ja erilaisien hyökkäystekniikoiden käyttöä.

ABSTRACT

Marko Lehtonen: Data manipulation in a cyber attack
Tampere University of Technology
Bachelor thesis, 25 pages
October 2017
Pervasive computing Bachelor's degree program
Major: Software Engineering
Examiner: University teacher Marko Helenius

Keywords: cyber, data, attack, manipulation

Cyber attacks have taken place in data networks for a long time. The most common way to attack is either to lock computer or steal user's data. The new threat to data is that it is modified from the original. In this way, critical systems can be set to operate wrongly or even break them. While such attacks have not yet been documented, at least in publicly, threat to data manipulation attack has increased.

The aim of this work was to find out what kind of threat manipulation of the data is and what things via data manipulation attack can be achieved. The thesis also examines the potential attackers' profiles and targets. Information about the attacks and the threat was largely collected from cyber security publications and studies. The information is used in this work to authenticate threats and evaluating the effects of the attack.

The study showed that the risk of data manipulation attack is real. Attack requires the attacker adequate resources, so that the attack can be useful. However, in the same time it was found that attack takes time and needs other techniques to succeed.

ALKUSANAT

Tämä kandidaatin työ on opettanut minulle uusia asioita kybermaailmasta. Nykyisessä yhteiskunnassa verkkoon siirretään yhä enemmän palveluita ja laitteita helpottamaan sekä ihmisten elämää, että yhteiskunnan toimintaa. Tietoa eli dataa kerätään samalla aina vain enemmän käyttöä ja analysointia varten. Tätä tietoa voidaan käyttää hyvään mutta samalla avoin järjestelmä antaa mahdollisuuden datan väärinkäyttämiseen tai sen manipulointiin.

Haluan kiittää tuesta ohjaajaa Marko Heleniusta sekä kaikkia työssä avustaneita henkilöitä aina aiheen antamisesta oikoluvussa auttamiseen. Lisäksi haluan erityisesti kiittää koko perhettäni opiskelujeni ajalta.

Tampereella, 29.10.2017

Marko Lehtonen

SISÄLLYSLUETTELO

LYHENTEET JA MERKINNÄT

DAESH	ISIS, jihadistijärjestö
DoD	Department of Defence, Yhdysvaltain puolustusministeriö
IoT	Internet of Things, laitteiden internet
Nasdaq	National Association of Securities Dealers Automated Quotations, arvopaperipörssi
NATO	North Atlantic Treaty Organisation, poliittinen ja sotilaallinen liittouma
OSINT	Open Source Intelligence, julkisten lähteiden tiedustelu
SIGINT	Signal Intelligence, signaalitiedustelu
SIRPNet	Secret Internet Protocol Router Network, luotettu verkko
ST luokitus	Suojaustaso, IV käyttörajoitettu, III luottamuksellinen, II salainen ja I erittäin salainen
UAV	Unmanned Aerial Vehicle, miehittämätön ilma-alus
VPN	Virtual Private Network, virtuaalinen erillisverkko

1. JOHDANTO

1.1 Yleistä

Sähköisen tiedon eli datan määrä ja arvo on kasvanut jatkuvasti. Samalla rikollisuus ja muu väärinkäyttö on laajentunut koskemaan myös tietoverkoissa liikkuvaa ja tallennettua dataa ja tietoa. Yleisimmissä hyökkäyksissä data lukitaan tai varastetaan käyttäjältä, tai data rikotaan käyttökelvottomaksi. Uudentyyppinen hyökkäystapa on muokata eli manipuloida dataa siten, että se näyttää oikealta tai ehjältä olematta sitä.

Tämän työn tutkimusongelma on se, miten ja mihin kohteisiin datamanipulaatiota voitaisiin käyttää verkkohyökkäyksessä. Samalla tarkastellaan keitä hyökkääjät voivat olla. Työn tavoitteena on antaa jokin arvio, siitä voiko hyökkäys tapahtua lähitulevaisuudessa.

Datan manipulointi on uusi tapa, perinteisempien datan varastamisen ja datan hävittämisen rinnalle. Hyökkäystavassa hyökkääjä pyrkii muuntamaan dataa niin, että sen käyttö aiheuttaa väärää toimintaa, rikkoo käyttäjän struktuuria tai aiheuttaa uhkaa tai vahinkoa henkilöille. Tällaista kohdennettua tapaa ei ole ennen käytetty hyökkäyksissä, mutta sen uhka on noussut esille keskusteluissa ja ennustuksissa puhuttaessa tulevaisuuden kyberuhista. Joissakin maissa uhasta on puhuttu avoimesti ja se on nostettu esille perinteisten hyökkäystapojen rinnalle valtiollisissa uhkakuvissa. Yhdysvaltain puolustusministeriön (DoD) vuoden 2015 kyberstrategiassa mainitaan tiedonmanipulointi esimerkiksi sairaaloiden terveyskertomuksien osalta [1].

Kyberhyökkäyksen, jonka yksi muoto voi siis olla data manipulointi, on hyökkääjälle houkutteleva ase. Verkossa tapahtuvat hyökkäykset tarjoavat eri tasoista näkymättömyyttä ja hyökkäyksien käsittely kansainvälisessä oikeudessa on epäselvää. Ei ole vielä olemassa sellaista selvää säännöstöä, jossa kyberhyökkäyksen voitaisiin sanoa vastaavan aseellista hyökkäystä, vaikka kyberhyökkäyksellä saataisiinkin aikaan samanlaista vahinkoa. Tällöin hyökkäyksen uhri ei voi käyttää kineettistä vastaiskua, niin että se olisi oikeutettua muiden silmissä. [2] Tämä houkuttaa kybertoimintaan erityisesti valtioiden välillä, niin sanotun harmaan vaiheen aikana, jolloin valtiot eivät ole vielä sodassa keskenään. Kybersodan ja teollisuushaitanteon osalta vakoilu on jo aiemmin siirtynyt verkkoon, sillä suuri osa valtioiden ja yritysten tiedoista on tallennettuna tietoverkkoihin ja useat ansaintalogiikat perustuvat tiedonkäsittelyyn.

Datamanipulaatio on yksinkertaisimmillaan sitä, että jonkin sensorin antamaa tietoa muutetaan todellisuudesta poikkeavaksi. Esimerkkinä tällaisesta yksinkertaisesta laitteen antaman datan manipuloinnista toimii vaikkapa lämpötila-anturin tiedon muuttaminen. Jos

jossakin järjestelmässä on sensori joka mittaa esimerkiksi nesteen lämpötilaa ja muun laitteiston toiminta riippuu tämän nesteen lämpötilan arvosta, voidaan dataa manipuloida siirtämällä anturi johonkin muuhun lämpötilaan. Tämä voi tapahtua siirtämällä anturi pois nesteestä ilmaan tai johonkin toiseen aineeseen, jossa on eri lämpötila kuin varsinaisessa kohteessa. Tällä tavoin saavutetaan saman tyyppinen lopputulos kuin murtautumalla syvälle järjestelmään ja muokkaamalla tietoja siellä. Aina tällainen yksinkertainen toteutus ei kuitenkaan ole mahdollista, vaan sensori voi olla saavuttamattomissa esimerkiksi niin, että se on fyysisesti suojattu kameroin, vartion tai muutoin rakenteellisesti, estäen hyökkääjän pääsyn sensorin läheisyyteen. On myös mahdollista, että järjestelmässä on tietoa keräämiä sensoreita niin paljon, ettei yhden lähettimen virheellinen data vielä aiheuta virheellistä toimintaa järjestelmässä.

Tämä työ alkaa mahdollisten hyökkääjien esittelystä, tämän jälkeen tarkastellaan mahdollisia hyökkäyksen kohteita sekä siviili- että sotilaskohteissa. Tämän jälkeen tarkastellaan lyhyesti mahdollisia tapoja suorittaa hyökkäyksiä, sekä niiltä suojautumista. Lopuksi tarkastellaan yhteenvetona kokonaisuutta hyökkäyksestä ja sen vaikutuksia.

2. PERUSTEET

2.1 Määritelmiä

Datan määrä on moninkertaistunut nykymaailmassa. IDC:n vuoden 2014 tutkimuksen mukaan digitaalinen universumi kaksinkertaistuu joka vuosi ja tulee kymmenkertaistumaan vuosien 2013 ja 2020 aikana [3]. Aiemmin fyysisen muistin ollessa rajattua ja kallista, dataa kerättiin vain niiltä osin, kuin sitä järjestelmässä tarvittiin. Nykyhetken suuntautumisena on kuitenkin kerätä mahdollisimman paljon dataa ja säilöä sitä käyttöä varten. Tästä esimerkkinä ovat tietotekniikan trendit, kuten datan louhinta, big data ja pilvipalvelut.

Koska dataa varten tarvitaan edelleen fyysistä muistia, data tallennetaan pilvipalvelun nimissä sopiviin datakeskuksiin tai vastaaviin paikkoihin, joihin käyttäjät ovat yhteydessä verkon ylitse. On myös mahdollista rakentaa verkko niin, että laitteet verkottuvat keskenään ja jakavat tiedon samassa verkossa olevien kesken. Usein tällaisissakin tapauksissa löytyy jokin piste, jonka kautta ohjataan ja kierrätetään dataa esimerkiksi, kun halutaan lähettää päivityspaketteja verkon laitteille. Data on kuitenkin aina olemassa jossain, joko hajautetusti laitteissa tai keskitetysti isommissa datavarastoissa. Se voi olla myös olla matkalla siirtotiellä.

Kyberillä tarkoitetaan tässä työssä koko digitaalista maailmaa. Siihen kuuluvat niin tietoverkot kuin -järjestelmät, ohjelmistot, internet ja kaikki, mitä voidaan kuvata bittien maailmana. Toisin sanoen se on kaikki muut paitsi fyysinen osa tietotekniikasta. Kyber-sanalla voidaan myös viitata fyysisen ja digitaalisen maailman rajapintaan. [4]

Data tarkoittaa tässä työssä tietoa, esimerkiksi 1 ja 0, jolla ei välttämättä ole itsessään semanttista tai informatiivista merkitystä. Jos datalla on semanttinen merkitys, se on tietoa. Dataa on olemassa erilaisissa muodoissa eri ympäristöissä. Tässä kirjoituksessa data tarkoittaa bittejä, joita käytetään tietotekniikassa.

Datan manipulointi tarkoittaa tässä työssä sitä, että varsinaista eli järjestelmässä käytettävää tietoa eli dataa manipuloidaan näyttämään toiselta, kuin mitä esimerkiksi fyysiset sensorit ovat sitä lähteestä alun perin keränneet. Manipulointi kohdistetaan johonkin haluttuun dataan, jotta saadaan vaikutettua järjestelmään piilossa. Loppukäyttäjä käyttää tätä muunnettua tietoa päätöksentekemiseen tai järjestelmän tai kokonaisen systeemin ohjaamiseen. Tämä toiminta voi olla esimerkiksi koordinaattien siirtoa, jonkin laitteen tai tapahtuman ohjaamista tai muuta vastaavaa toimintaa. Manipulointi voidaan suorittaa useassa kohdassa datan elinkaaren ja liikkeen aikana. Dataa voidaan muokata sen lähtöpisteessä, siirtämisen aikana tai datan tallennuspaikassa. Hyökkäystekniikka valitaan sen

mukaisesti, missä kohdassa manipulointi suoritetaan. Manipulointi ei siis tässä työssä tarkoita loki tai muiden vastaavien tiedostojen muuntamista niin, että esimerkiksi hyökkäyksestä ei jää jälkeä. Tällainen toiminta on osa hyökkäyksen salaamista.

Datan manipulointi tulee erottaa perinteisemmästä tiedon muuttamisesta, jota käytetään esimerkiksi propagandana. Tällöin puhutaan disinformaatiosta. Tällaisessa tapauksessa kyseessä on pikemminkin väärän tai harhaanjohtavan tiedon antaminen.

2.2 Kyberhyökkäyksen ominaisuuksia

Datamanipulointia voidaan käyttää esimerkiksi sellaisessa tapauksessa, kun ei haluta jättää suoraa jälkeä toimijasta. Mikäli dataa manipuloidaan onnistuneesti, vaikutukset voivat näkyä vasta jonkin ajan kuluttua. Tämä tapahtuu, kun virheellinen data on kertautunut tarpeeksi järjestelmän sisällä, tai kun laitetta käytetään jonkin määrätyn tehtävän suorittamiseen. On tosin mahdollista, että vikaantuminen tapahtuu samalla hetkellä, kun dataa käytetään ensimmäistä kertaa. Tarkan hyökkäyksen suorittamiseksi hyökkääjän olisi tiedettävä tarkasti järjestelmän toiminnallisuus ja sen sisältämän datan ominaisuudet. Koska suuressa järjestelmässä voi olla paljon epäsäännöllisyyttä hyökkääjän näkökulmasta, tai siinä voi olla useita vaikuttavia elementtejä, tarkan tiedon arviointi tai tietäminen on yleensä vaikeaa, ainakin ilman täydellisiä dokumentteja. Tästä johtuen hyökkäyksen vaikutus ja vaikuttamisaika voivat vaihdella suuresti.

Valveutuneelle puolustautujalla on olemassa useita suojamekanismeja valmiina omassa järjestelmässään. Data suojataan yleensä hyvin, sillä se on usein yksi tärkeimmistä asioista yritykselle tai valtiolle. Data pyritään eristämään muusta verkosta, mutta koska sitä on käytettävä, on siihen kuitenkin olemassa jonkinlaisia yhteyksiä ulkoverkosta. Dataa suojataan sen siirron aikana esimerkiksi VPN-yhteyksillä tai muilla turvallisilla verkkoratkaisuilla. Joissain tapauksissa, varsinkin vanhemmissa infrastruktuureissa, voi kuitenkin olla mahdollista, että suojaus on jäänyt heikommaksi tai puutteelliseksi joissain yksittäisissä kohdissa. Voi olla myös mahdollista, että sensorien luona on heikompi fyysinen suojaus ja dataa on mahdollista päästä manipuloimaan jo sen alkulähteellä. Tällaisia heikomman suojauksen kohteita voisivat olla esimerkiksi jonkinlaiset jakelupisteet, jotka sijaitsevat kauempana muista järjestelmän osista ja joissa ei ole henkilöstöä jatkuvasti valvomassa.

Datan varastointipaikoissa data säilytetään yleensä kryptattuna haltijan omissa tiloissa. Salaaminen kuuluu perustoimenpiteisiin tiedon säilyttämisessä. Tällä tavoin pyritään estämään sen käyttäminen, mikäli joku pääsee järjestelmään sisälle. On kuitenkin mahdollista, että yritys antaa datansa kolmannen osapuolen haltuun varastoitavaksi. Näin yritys säästää omissa tallennus- ja varmuuskopiointikustannuksissaan. Tällainen järjestely ei kuitenkaan välttämättä paranna tietoturvaa, vaan data on samalla tavalla hyökkääjän saavutettavissa kuin se olisi tallennettuna omistajansa haltuun.

Internetin käytön yleistyessä koko maailmassa erilaisia laiteita liitetään tai suunnitellaan liitettäväksi verkkoon yhä enemmän. Tietoliikenne- ja elektroniikkayritys Cisco arvelee, että vuoteen 2020 mennessä 50 miljardia laitetta olisi kytkettynä internetiin ja vuonna 2012 kytkettyjen laitteiden arvioitu määrä olisi jo 8.7 miljardia. Suuntaus on sama sekä siviili- että sotilaslaitteissa ja järjestelmissä. Siviilipuolella puhutaan laitteiden internetistä, johon halutaan kytkeä mitä erilaisimpia laitteita valvontakameroista jääkaappeihin. Sotilasjohtamisjärjestelmissä halutaan ajantasaista tietoa erilaisilta sensoreilta ja muilta informaatiolähteiltä. Molemmissa tapauksissa yksi ratkaisu rakentaa tällaista infrastruktuuria on käyttää avoimia rajapintoja, jotka mahdollistavat laitteiden lisäämisen helpommin järjestelmään. Tämä kuitenkin aiheuttaa mahdollisen tietoturvaongelman. Avointa rajapintaa voi olla mahdollista käyttää väärin, mikäli sen suojauksista ei ole huolehdittu oikein tai sitä ei päivitetä. Tällöin voidaan käyttää joko itse laitetta tai laitteen kautta dataa väärin. Erityisesti luokiteltujen laitteiden osalta tulee ongelma, mikäli verkkoon liitettävissä oleva laite päätyy vääriin käsiin eikä tätä huomata ajoissa. Tällöin jokin luotettavaksi luultu laite pääsee muuttamaan dataa suojatussa tai suljetussa järjestelmässä.

3. HYÖKKÄÄJÄN PROFIILI JA MOTIVAATIO

Kyberhyökkääjät voidaan karkeasti viiteen eri toimijaan, jotka esitellään tämän luvun alakohdissa. [4] Jokainen näistä toimii omalla tavallaan ja jokaiselle voidaan päätellä motivaatio toimintaansa. Jaottelun voisi tehdä muullakin tavalla, mutta tämä jaottelu kattaa hyvin pääosan tapauksista. Aina on mahdollista olla jokin yksittäinen toimija, joka ei suoraan mahdu alla oleviin kategorioihin tai voisi toimia useassa ryhmässä.

Taulukko 1 Hyökkääjien erittely.

	Motivaatio	**Kohde**
Krakkerit ja yksinäiset sudet	Julkisuus, poliittinen, kosto	Henkilöt, yritykset, valtio
Rikolliset	Raha, julkisuus, kiristys	Henkilöt, yritykset
Terroristit	Julkisuus, raha, kiristys	Henkilöt, valtiot, yritykset
Yritykset	Vakoilu, sabotointi, kiristys	Yritykset, henkilöt
Valtiot ja valtioiden avustamat	Vakoilu, kybersota, haitanteko	Valtio, kriittiset järjestelmät, sotilaskohteet

3.1 Aktivistit ja yksinäiset sudet sekä krakkeriryhmät

Tähän luokkaan voidaan määritellä kaikki ne henkilöt, jotka toimivat yksin tai pienessä ryhmässä. Krakkeriryhmät voivat olla kuitenkin isoja ja levitä kansainvälisesti laajalle. Esimerkki tällaisesta ryhmästä on Anonymous. Yksittäisen henkilön tai hyvin pienen ryhmän (2-3 henkeä) motivaationa toimia verkossa jotain vastaan on yleensä nimen saaminen jossain yhteisössä, kuten esimerkiksi krakkeriyhteisössä tai poliittiset motiivit. Myös kosto jostain tapahtumasta, jota pitää henkilökohtaisena vääryytenä voi aiheuttaa sen, että kostotoimi halutaan tehdä verkossa. Tällaisten yksilön hyökkäyksen kohteena voi olla oikeastaan mikä tahansa, se voi olla hallitusta, yritystä tai toista yksilöä vastaan tehty.

Yleisesti ottaen krakkereiden ja koko haktivismi ideologian tarkoituksena on osoittaa muille jokin epäkohta ja toimia sitä vastaan. Joskus jopa laittomin keinoin. Kakkerit eivät

kuitenkaan aina toimi yksin, vaan jonkinlaisessa ryhmässä ja se erottaa tämän edellä mainituista yksinäisistä toimijoista. [5]

Kummassakin tapauksessa lähes aina tällaiset henkilöt tai ryhmät haluavat jättää toiminnastaan jonkinlaisen merkin. Tällä tavoin heidän sanomansa saa näkyvyyttä koko maailmalle. Datan manipulointia voisi olla mahdollista käyttää näissä tapauksissa. Sillä tavoin voisi antaa signaalin, että vastustaja eli tässä tapauksessa hyökkääjä, on teknologisesti vahva ja taitava. Kuitenkin datan manipulointi ei anna tällaiseen kovinkaan hyvää työkalua. Hyökkäys voi olla vaikea suorittaa ja lisäksi tulokset eivät ole välttämättä kovinkaan ennustettavia. Varoituksen antamiseen tai voimannäyttöön riittää tavallinen tiedostojen rikkominen tai tiedon varastaminen. Samoin voi olla mahdollista, että hyökkääjä jää kuuntelemaan ja vakoilemaan järjestelmässä kulkevaa tietoa. Silloin on parempi toimia salassa ja koittaa piilottaa oma toimintansa.

3.2 Rikolliset

Rikollinen toiminta on aina liikkunut hyvin nopeasti uusien tekniikoiden mukana. Tämä on tapahtunut myös tietotekniikan mukana ja avulla. Rikollisten lähes ainut motivaatio toiminnassaan on rahan saaminen. Se miten rahaa kerätään, vaihtelee ja saattaa tapahtua kiertotietä. Rikollisryhmän tavoitteena saattaa olla myös kerätä ensin mainetta ja vasta sitten tai sen avulla saavuttaa rahallista hyötyä. Keinoina tietotekniikassa on viime aikoina ollut kiristäminen. Erilaisten haittaohjelmien avulla käyttäjien koneita saatetaan lukita tai yrityksiä yritetään vakoilla tai kiristämisellä ja salaisuuksien myymisellä saada rahaa.

Datan manipulointi ei näissä tapauksissa ole kovinkaan todennäköistä. On helpompaa tunkeutua tietojärjestelmään tai yksittäiselle koneelle ja varastaa tietoa tai lukita kone. Tällä tavoin hyökkääjän ei tarvitse erikseen murtaa mahdollisesti kryptattua dataa tai tutustua siihen, miten dataa käytetään. Näin vähemmillä resursseilla saavutetaan sama hyöty. Vain James Bond tyyppisissä tapauksissa voitaisiin kuvitella, että rikollinen manipuloi dataa kiristämistarkoituksissa.

3.3 Terroristit

Terrorismilla tarkoitetaan tässä kohtaa laittoman väkivallan ja pelottelun käyttämistä, erityisesti siviilejä vastaan, poliittisten tavoitteiden saamiseksi. Näin myös Oxfordin sanakirja määrittelee asian [6]. Ja samalla voidaan todeta, että terroristi on henkilö, joka toimii edellä mainitun määritelmän tavoin. Määritelmä ei itsessään ole kiistaton, ja siitä väitellään katsantosuuntien mukaan.

Terroristien motivaationa on pääasiallisesti siis poliittisen huomion saaminen, mutta samalla järjestäytyneet terroristiorganisaatiot tarvitsevat rahaa toimintaansa. Huomiota haluttuun epäkohtaan voidaan hakea valtion tai lähivaltioiden sisällä, mutta vahvoilla järjestöillä voi olla tavoitteena huomion hakeminen maailmanlaajuisesti.

Terroristien toiminnan kohteina ovat yleensä infrastruktuuri, maan erilaiset voimavarat, kuten esimerkiksi turismi tai teollisuus sekä julkiset kohteet. Julkisista kohteista erityisesti hallinnon omistamat tai huolehtimat kohteet ovat houkuttelevia hyökkäykseen.

Dataan kohdistuvat hyökkäykset ovat mahdollisia, mutta eivät todennäköisiä. Kyberhyökkäyksellä olisi mahdollista saada aikaan suurta näkyvääkin vahinkoa ja aiheuttaa paniikkia väestön keskuudessa. Hyökkäys ei vaadi samanlaisia rahallisia resursseja kuin yleensä kineettiset hyökkäykset. Mutta se vaatii hyökkääjältä suurempaa teknistä osaamista ja teknisiä resursseja. Joillain järjestöillä voisi olla mahdollista hankkia sopivia ja päteviä henkilöitä. Esimerkiksi DAESH-järjestöllä on käytössään runsaasti tietotekniikkaa ja jopa omia tietoteknisiä palveluita.

Hyökkäyksen toteuttaminen ei kuitenkaan ole helppoa. Yleisesti ottaen terroristeilla on tapana käyttää perinteisiä tapoja hyökkäyksien toteuttamiseen. Vaikka tekninen kehitys on edennyt ja on mahdollista hankkia kaupallisia laitteita erilaisten iskujen suorittamiseen, kuten vaikkapa lennokkeja, ei niitä ole nähty toiminnassa. Vasta vuonna 2016 DAESH suoritti hyökkäyksen käyttäen hyväkseen lennokkeja, vaikka tekniikka on ollut kaupallisesti saatavilla jo useita vuosia [7].

Verkkohyökkäyksen suorittaminen vaatii siihen sopivan infrastruktuurin. Hajallaan asutuissa tai suljetuissa valtioissa verkon tarkkailu on helpompaa ja vähäisestä liikenteestä on helpompi erottaa mahdolliset hyökkääjät. Maissa joissa terroristit ovat toimineet jo pidempään usein valtio jo osaa valvoa verkkoaan osana signaalitiedustelua (SIGINT).

3.4 Yritykset

Todennäköisin kohde yrityksen suorittamalle kyberhyökkäykselle on toinen yritys. On kuitenkin vaikea uskoa, että yritys toimisi toista vastaan manipuloimalla sen sisäistä dataa. Markkinoista kilpailtaessa todennäköisin toiminta kyberympäristössä on joko yritysvakoilu tai vähäisemmässä määrin kiristäminen. Myös kosto voisi olla mahdollinen joissain tapauksissa. Näin ajateltaessa yrityksen toimien kohteena olisi siis toinen yritys, mutta se voisi toimia myös kohdeyrityksessä työskentelevää yksilöä vastaan. Yksilön vakoilu tai kiristäminen toimisi keinona vaikuttaa kilpailevaan yritykseen kiertotienä. Mikäli yrityksen toimintaa tukee tai peittelee jokin hallituksen suoja, se saattaa toimia eri tavalla. Tällöin vakoilua voitaisiin tukea ja kiinni jäädessään yritystä tuetaan niin, että haittavaikutukset jäisivät mahdollisimman pieniksi. Tällaista toimintaa ei kuitenkaan käsitellä tässä työssä tämän enempää.

Kun yritykset toimivat toisiaan vastaan, ilman valtion tai vastaavan tukea, todennäköisin toiminnan motivaatio on siis yritysvakoilu. Äärimmäisessä tapauksessa voitaisiin kuvitella, että yritys haluaisi sabotoida toista yritystä muokkaamalla tämän pilvipalvelussa olevaa dataa. Tällainen kohde voisi olla jonkin tuotteen testi- tai laboratoriotuloksien datan manipuloiminen. Näin yritettäisiin saada oma tuote halutummaksi tai ostaa aikaa oman tuotteen kehittämiseen. Kummassakin tapauksessa datan varastaminen tai sen hävittäminen toimisivat samalla tavoin ja helpommin metodein. Toinen tapa voisi olla yrityksen rahatietojen datan manipulointi. Tällä keinolla olisi mahdollista vaikuttaa yrityksen talouteen ja sillä tavoin haitata sen toimintaa tai jopa ajaa yritys konkurssiin.

Suurilla yrityksillä voisi olla tekniset mahdollisuudet ja sekä henkisiä, että rahallisia resursseja, mutta riskit ovat suuret. Kiinni jäädessään vakoilua tai muuta haittaa tehneen yrityksen julkisuuskuva heikkenee ja vaikuttaa tuotteen ostajiin. Lisäksi yritykset suojaavat omat tietonsa yleensä hyvin ja tarkkailevat omaa verkkoaan hyökkääjien varalta. Tämän vuoksi yrityksen, ainakin sen toimiessa yksinään, todennäköisyys manipuloida dataa on melko pieni.

3.5 Valtiot ja valtion sponsoroimat joukot

Tässä kappaleessa käsitellään valtion joukkoja ja yksiköitä sekä sellaisia joukkoja jotka toimivat valtion mandaatilla, vaikkakin ilman näkyvää yhteyttä valtioon. Periaatteessa sellaisia voisivat olla myös yritykset, mutta mikäli ne toimivat omasta intressistään ollen vain valtio suojeluksessa, niiden toiminta liittyy kappaleeseen 3.4.

Valtio todennäköisimmin hyökkää toista valtiota vastaan. On mahdollista osallistua myös yritysvakoiluun tai suosia haluttuja toimijoita teollisuuden ja kaupan alalla. Tällaisia tapauksia on ollut kautta historian. Kauppatarjouksia on vuotanut kilpailijoiden tietoon liian aikaisin ja tiedon saanut on voinut korjata omaa tarjoustaan niin, että sen valinta on ollut todennäköisempää. Erilaiset Leaks-sivustot, kuten tunnetuimpana WikiLeaks, ovat esittäneet tällaisia dokumentteja ja tietoja ainakin vuodesta 2015 alkaen.

Motiivina kyberhyökkäykselle toiseen valtioon ovat samat kuin konventionaalisessakin toiminnassa. Rauhan aikana vakoillaan, jotta tiedetään mitä toinen on tekemässä. Poliittinen toiminta korostuu aina välillä, kun kohdemaan poliittisessa elämässä tapahtuu jotain tärkeää. Vuoden 2016 Yhdysvaltain presidentin vaalien alla Venäjän on syytetty sekaantuneen erilaisiin hakkerointi tapahtumiin, johdatellakseen vaalien tulosta haluamaansa suuntaan. Samanaikaisesti Yhdysvallat varautui siihen, että elektronisiin äänestyslaitteisiin voitaisiin tunkeutua ja siten muuttaa äänestystulosta.

Harmaan vaiheen ja kriisinaikana toiminnan kohteina ovat kriittiset ja strategiset kohteet. Kohteita voivat olla sotilaalliset kohteet, kuten johto- tai viestijärjestelmät. Tai toisaalta kohteena voi olla yrittää vaikuttaa yhteiskunnan toimintaan liittyviin järjestelmiin ja kohteisiin. Tällaisia voivat olla jo aiemmin mainitut sähköjakelu tai sairaalat.

Ennustetaan, että tietoverkoissa tapahtuvat konfliktit tulevat kasvamaan. Asymmetrisiä konflikteja, joissa korkeamman teknologian omistava pyrkii vaikuttamaan heikompaan osapuoleen, on nähtävissä tulevaisuudessa informaatiosodankäynnissä, johtamissodankäynnissä ja elektronissa sodankäynnissä. Asymmetriset iskut eivät tosin vaadi sitä, että toinen on heikompi osapuoli tietotekniikassa. Edellä mainitut sodankäynnin tekniikat ovat kuitenkin vain uusia keinoja ja tapoja vaikuttaa järjestelmiin, eikä niillä voida kuitenkaan suoraan korvata perinteisiä menetelmiä [8].

Datamanipulaation käyttäjä on kuitenkin todennäköisimmin valtiollinen toimija. Sillä on saatavissaan erilaisia resursseja ja riittävästi tukea toimintaansa. Lisäksi datan manipuloinnista on eniten hyötyä iskuissa, jotka voidaan suorittaa valtion hyödyksi.

4. DATA MANIPULAATION KOHTEITA

4.1 Kriittisiä siviilikohteita

Mikäli yhteiskunta halutaan sekoittaa, kohteita löytyy useita erilaisia. Monet nykyaikaiset järjestelmät ovat usein automatisoituja ja niitä saattavat hoitaa robotit tai pelkästään ohjelmistot. Ihmisen tehtävänä on tarkkailla järjestelmää ja toimia vasta, kun järjestelmä hälyttää tai muutoin huomata toiminnan olevan prosessin vastaista tai epäilyttävää.

Kriittisiä järjestelmiä yhteiskunnassa ovat muun muassa sähkönjakeluverkot, sairaaloiden järjestelmät tai vaikkapa pörssi, jonka heilahdukset näkyvät nopeastikin yhteiskunnan ja yritysten toiminnassa. Mikäli joku pääsisi muokkaamaan sähkönjakeluverkon tietoja se saattaisi joko ylikuormittaa alueita tai laitteita tai keskeyttää jakelun kokonaan. Sairaalan järjestelmässä datan muokkaaminen voisi saada aikaan sen, että elektronisten reseptien käyttäjät saisivat toistensa lääkkeitä. Mikäli käyttäjät tai henkilökunta eivät tiedä oikeaa lääkemääräystä voi kestää hetken, ennen kuin ongelma havaitaan ja vakavimmassa tapauksessa voidaan menettää jopa henkiä.

Siviilijärjestelmien yksi erikoistapaus on se, että data sijaitsee jonkun toisen yrityksen hallussa, jolta on ostettu datan säilytyspalvelu tai sitä käyttää jokin kolmas osapuoli. Tällainen järjestely voi tapahtua ilman että käyttäjä kiinnittää asiaan edes huomiota. Tällaisia ylläpitojärjestelmiä ovat mm. pilvipalvelut. Jossain pilvessä olevaa dataa voidaan käyttää vaikkapa puhelimen applikaatiolla, jonka on valmistanut kolmas osapuoli. Vaikka varsinaisesti pilveen ei suoraan murtauduttaisikaan voisi hyökkääjä käyttää tätä applikaatiota murtautumisvälineenä. Tällä hetkellä kasvava järjestelmä on erilaisten laitteiden liittäminen internettiin. Monet näistä laitteista tukeutuvat kolmanteen osapuoleen, joka välittää tietoa tai tarkkailee sitä jonkin lisäpalvelun nimissä.

Järjestelmää, jossa laitteita liitetään verkkoon, kutsutaan yleisesti nimellä IoT (Internet of Things). Siinä erilaiset laitteet keskustelevat esimerkiksi keskenään internet verkon ylitse tai ovat yhteydessä verkon kautta käyttäjäänsä tai omistajaansa. Yksittäisenä laitteen datan manipulointi tuntuu vähäpätöisenä IoT:ssä, mutta kun laitteet verkottuvat keskenään niiden jakaman datan muokkaaminen voi aiheuttaa suurempia ongelmia. Esimerkkinä voidaan kuvitella tapahtuma, jossa ajoneuvot jakavat tietoa keskenään liikennetiedoista. Datan voisi manipuloida näyttämään ruuhkaa johonkin pisteeseen, jolloin todellinen ruuhka muodostuu muualle. Tätä keinotekoista ruuhkaa voidaan sitten käyttää hyväksi johonkin toiseen toimintaa tai haittaamaan viranomaisten tai pelastuspalvelun toimintaa. Tällaista liikenteeseen liittyvää hyökkäystä ei vielä ole todennettu, koska käyttäjiä ei ole vielä niin paljon. Kuitenkin vuoden 2017 automalleissa ja navigaattorivalmistajien laitteissa on olemassa ominaisuuksia, joilla voidaan kuljettajaa varoittaa ruuhkista matkalla ja samalla ehdotetaan uutta reittiä. IoT-laitteita on käytetty vuoteen 2017 mennessä jo

onnistuneisiin DOS -hyökkäyksiin bottiverkossa sekä erilaisiin rahan keräyksiin ja kiristykseen. Useita saman valmistajan valvontakameroita on esimerkiksi saatu suorittamaan hyökkäys ohjelmistovirheen ansiosta. Laitteiden tietoturva oli ollut puutteellinen, jolloin hyökkääjän oli mahdollista käyttää laitteiden internet yhteyttä omiin tarkoituksiinsa.

Dataan kohdistuvan hyökkäyksen ei kuitenkaan tarvitse vaikuttaa heti. Tilanteessa, jossa hyökkääjä iskee yritykseen, joka huolehtii toisen yritysten rahavirroista, voi saada pahempaa tuhoa aikaiseksi, kun muutos saadaan tapahtumaan kertautumalla. Muokkaamalla dataa niin, että muokkaus tapahtuu vaikkapa päivittäin ja sopivasti ennen vuosi- tai neljänneskatsauksia asiakkaat eivät huomaa tapahtunutta ajoissa. Mikäli hyökkääjä pääsee toimimaan näin, ei järjestelmän palauttaminenkaan onnistu helposti yhdellä palautuskerralla, vaan muutokset on otettava huomioon jokaiselta muutoshetkeltä. Palauttaen varmuuskopio askel tai päivä kerrallaan kohti hyökkäyksen aloitushetkeä. Tällainen palauttaminen ja siihen liittyvä testaus ei tapahdu nopeasti, vaan asiakkaiden tilit ja saldot ovat mahdollisesti jäädytettyinä pitkän aikaa.

Tällainen toiminta voisi tapahtua erityisesti harmaanvaiheen aikana, eli hetken ennen varsinaista kriisiä. Tällöin voidaan aiheuttaa häiriöitä markkinoilla ja yhteiskunnan toiminnassa, haitaten edellä mainittujen toimintamekanismien normaalia toimintaa.

4.1.1 Pörssi ja virtuaalinen varainhoito

Pörssiin kohdistuva hyökkäys voisi olla yksi eniten rahallista haittaa aikaan saava isku. 2016 Visual Capitalist lehden mukaan 60:n suurimman pörssin yhteisarvo oli 69 biljoonaan dollaria [9]. Nykyisin suurissa pörsseissä ainakin osan kaupasta käyvät jo robotit. Tätä nimitetään virtuaaliseksi varainhoidoksi ja sen englannin kielinen termi on robo advising. Kevyimmillään algoritmit ehdottavat käyttäjälle kauppoja, mutta koko salkun hoitaminen eli ostaminen ja myyminen voidaan siirtää virtuaalisen järjestelmän hoidettavaksi. Virtuaalista varain hoitoa on käytössä internet lähteiden mukaan Yhdysvalloissa, jossa se on yleisintä, mutta myös Australiassa, Intiassa, Kanadassa ja Euroopassa.

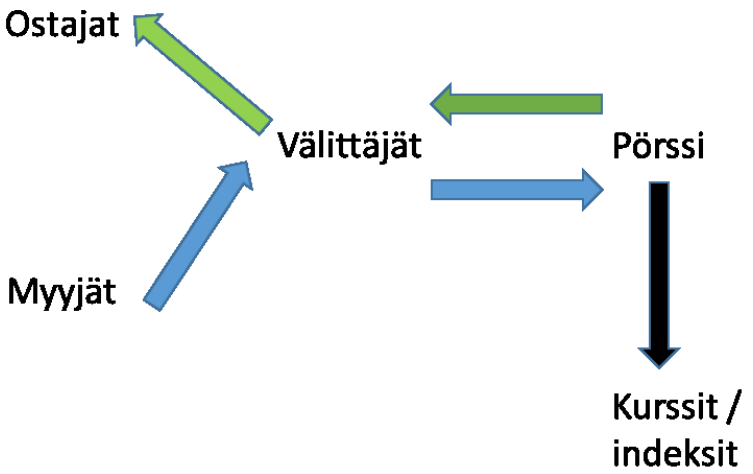
2014 MyPrivateBankingin tutkimuksen mukaan kyseisen vuoden lopussa arvioitiin robottien hallinnassa olevan 14 miljardia dollaria ja samaisen tutkimuksen arvio oli, että viidessä vuodessa, eli vuoteen 2019 arvo kasvaisi 255 miljardiin dollariin [10]. Vaikka vielä sijoitetun rahan määrä suhteessa kaikkeen sijoitettuun rahaan on pieni sen osuus kasvaa ennusteen mukaan hyvin nopeasti.

2013 Kiinassa Shanghain pörssissä keskeytettiin China Everbright Securities yrityksen kaupankäynti. Yrityksen robotti, joka suoritti kaupankäyntiä, yritti ostaa osakkeita 2,86 miljardilla eurolla. Ennen ostamisen estämistä robotti oli ehtinyt ostamaan osakkeita alle 900 miljoonalla eurolla. [11] Tässä tapauksessa pörssin yleiskurssi oli kuitenkin noussut, eikä laskenut, mikä voisi olla hyökkääjän tavoite. Kuitenkin kun kurssit korjaantuvat voi

tapahtua tappioita muille Vastaavanlaisia ongelmia on tapahtunut muuallakin, mm. Nasdaq on keskeyttänyt kaupankäyntinsä ohjelmistovian takia, kun sen osakenoteerauksien ohjelmisto toimi väärin vuonna 2013.

4.1.2 Hyökkäys pörssiin

Pörssissä kaupankäynti tapahtuu ohjelmistojen avulla. Riippuen pörssin koosta ohjelmistojen merkitys vaihtelee, mutta yleisesti voidaan sanoa, että ohjelmistoja tarvitaan kaikkeen. Ohjelmat käyvät kauppaa, analysoivat tapahtumia markkinoilla ja niin edelleen. Voidaan kuvitella millaisia virheitä voisi saada aikaiseksi, jos näiden ohjelmien käyttämä data on manipuloitua, mutta kuitenkin sellaista joka saa ohjelmat jatkamaan toimintaansa. Pörsseissä käytetyissä ohjelmissa on tapahtunut ohjelmistovirheitä, joista johtuen on jouduttu keskeyttämään kaupankäynti. Kuva 1 Pörssin toimintaperiaate. on esitetty, millä tavoin pörssi toimii karkealla tasolla. Robotit toimivat ostajina ja myyjinä ja ohjelmistoja käytetään osallisena kaikissa pörssin toimintavaiheissa.



Kuva 1 Pörssin toimintaperiaate.

Koska markkinamaailma on, ainakin ulospäin jonkin verran, ennustamatonta datamanipulaation vaikutukset ovat myös ennustamattomia. Pörssin toimintaa, eli indeksejä valvotaan jatkuvasti ja samoin pörssissä tehtyjä osto- ja myyntitapahtumia valvotaan. Mikäli pörssissä tapahtuu jotain, mikä näyttää oudolta kaupankäynti voidaan keskeyttää.

Yksi mahdollinen tapa hyökätä pörssitoimintaa vastaan on etsiä sellainen yritys, joka suorittaa robottikauppaa pörssissä. Hyökkääjä voi hakkeroitua yrityksen verkkoon ja manipuloida dataa sen sisällä tavoitteena saada kaupankäynti sekaisin. Onnistuneen suorituk-

sen kannalta on tärkeää, ettei datan muokkausta havaita ennen kaupankäynnin aloittamista. Kolmannen osapuolen kautta suoritettu hyökkäys olisi varmasti todennäköisin keino toimia pörssimaailmassa. Mikäli hyökkääjä pystyisi vielä käyttämään samaan aikaan useampia robotteja datamanipuloinnissa, olisivat vaikutukset suuremmat.

4.2 Yleistä sotilaskohteista

Sotilaskohteisiin ja sotilasjärjestelmiin tunkeutuminen on yleisesti ottaen haastavaa. Järjestelmät pyritään eristämään ja suojaamaan hyvin. Lisäksi laitteet ja data ovat fyysisesti useimmiten vahvasti suojattuina. Jotta voitaisiin päästä sisään järjestelmään, tulisi päästä sisälle tukikohtaan ja rakennukseen ja siellä suoraan sellaisiin järjestelmän osiin tai laitteisiin, joista pääsee esimerkiksi suoraan tietokantaa käsittelemään. Tällaisessa tapauksessa voi olla toimintatapana hyökätä verkossa kulkevaan dataan.

Nykyaikaisessa sodankäynnissä tietoverkkojen ja tiedon siirtämisen merkitys yksiköiden välillä on kasvanut. Esimerkiksi hävittäjät voivat kommunikoivat keskenään ja vaikkapa ilmatorjunnan kesken jollakin datalinkkijärjestelmällä. Tällainen on esimerkiksi NATO:n käyttämä Link-16 -järjestelmä. Tietoa ja tilannekuvaa pitää voida jakaa reaali- tai lähes reaaliajassa yksiköiden kesken, jotta joukkoja voidaan suunnata haluttuun paikkaan ja samalla tunnistaa omat joukot ja estää vahingossa tapahtuvat hyökkäykset omiin henkilöihin (blue on blue tilanne).

Muita esimerkkejä sotilasjärjestelmistä ovat johtamis- ja tiedustelujärjestelmät, mutta niihin tunkeutuminen voi olla vielä haastavampaa kuin vaikkapa lennokkijärjestelmän ohjaukseen tunkeutuminen. Ajankohtaisesti F-35 koneen järjestelmä ei ole suljettu järjestelmä, vaan konetta on mahdollista päivittää jopa tehtävän aikana [12].

4.3 UAV

UAV:t eli miehittämättömät lennokit ovat nousseet yhä suurempaan rooliin taisteluissa. Niitä voidaan käyttää operaatioalueella erilaisiin tiedustelutehtäviin, kuten esimerkiksi kuva- tai signaalitiedusteluun (IMINT, SIGINT). Mutta myös vaikuttamaan vihollisen kohteisiin. UAV:den etuna on se, että konetta voidaan lennättää kaukaa ja näin mahdolliset omat tappiot rajoittuvat periaatteessa vain laitteeseen.

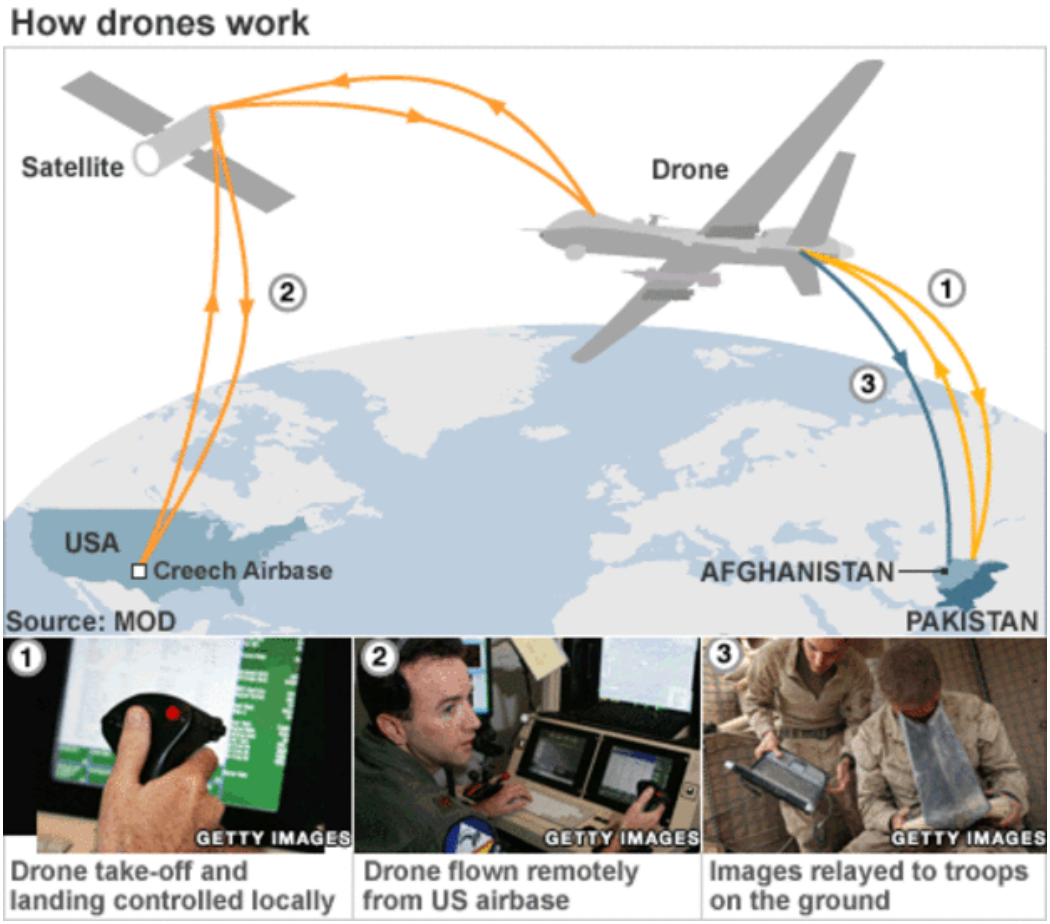
Toimittaessa kansainvälisessä tehtävässä, varsinainen laukaisu ja alkulennätys voidaan suorittaa paikallisesti, mutta varsinainen tehtävä voidaan hoitaa vaikkapa toiselta mantereelta. Tällöin muodostetaan ohjaamista varten yksi verkko, joka voi toimia vaikkapa satelliittiyhteyden ylitse ja mahdollisesti toinen, jolla voidaan siirtää kuvaa esimerkiksi toisella verkkoyhteydellä. Vaikka verkko pisteiden välillä on salattu ja suojattu, on hyökkääjällä mahdollista päästä verkkoon, viestijöiden väliin ja muuttaa dataa.

4.4 Hyökkäys lennokkijärjestelmään

Lennokkien ohjaus- tai toimintajärjestelmään iskettäessä pitää hyökkääjän miettiä, minkä kokoisesta laitteesta on kyse ja mihin sitä operaatiossa käytetään, valitakseen optimaalisen kohteen. Kevyitä lennokkeja tai koptereita ohjataan hyvin paikallisesti. Niiden toimintasäde on usein vain näkyvä alue eli line of sight (LOS). Tällaiseen järjestelmään on vaikea iskeä datamanipulaation keinoin. On helpompi tapa häiritä lähetyssignaalia, ja tällä tavoin rikkoa lennokki tai estää kuvan lähettäminen lennättäjälle.

Suurien lennokkien, kuten esimerkiksi MQ-9 Reaper:n, toimintatavat ja tarkoitukset ovat kuitenkin erilaisia. Koneiden lentomatkat lähentelevät tuhatta kilometriä ja lentoajat saatavat olla yli vuorokauden mittaisia. Ne voivat, koneesta riippuen, kantaa suurenkin asekuorman esimerkiksi useampia ohjuksia tai tiedustelulaitteita.

Koneen ohjaaminen voidaan tehdä usealla eri tavalla, ja tulevaisuudessa ne voidaan asettaa toimimaan autonomisesti. Darpalla on olemassa tämän suuntaisia projekteja käynnissä [13]. Mutta tällä hetkellä koneita voidaan lennättää esimerkiksi niin, että konetta ohjataan nousun ajan paikallisesti lähtökentältä johonkin sovittuun koordinaattipisteeseen tai -ruutuun sekä korkeuteen ja tämän jälkeen ohjaus vastuu annetaan muualle. Tämä muu voi sijaita operaatiosta riippuen toisessa valtiossa tai jopa toisella mantereella. Esimerkiksi Afganistanin operaatiossa keskikokoisia koneita, kuten MQ-B1 ja MQ-9 -koneita lennätetään Yhdysvaltain ilmavoimien Creechin tukikohdasta, Kuva 2 Lennokkijärjestelmän toiminta. Yhteys koneeseen muodostetaan sopivan sotilassatelliitin kautta ja viestintään käytetään suojattua SIRPNet verkkoa.



Kuva 2 Lennokkijärjestelmän toiminta.

Haavoittuvia kohteita on tällöin itse koneen ohjelmisto, data jota käytetään koneen noustessa, satelliitin kautta välitettävä data ja operaation aikaisen lennättämisen data. SIRPNetin on oletettu olevan turvallinen verkko, mutta vuonna 2016 useampi lennätys epäonnistui, mahdollisesti verkossa olevan ongelman takia. Koneet ovat iskeneet vääriin kohteisiin ja vahingoittaneet siviilejä. Tällaisia epäonnistuneita iskuja on tapahtunut operaatioissa eri taistelualueilla [14][15].

Hyökkäykseen voidaan olettaa käytettäväksi kahta erilaista tekniikkaa, toinen on niin sanottu välimieshyökkäystä, jossa data kaapataan verkossa matkalla lähettäjältä vastaanottajalle ja sen tietoja muutetaan ennen kuin se lähetetään vastaanottajalle. Tässä tapauksessa pitäisi päästä satelliitin tai satelliittien väliin, ottaa tieto vastaan ja manipuloida data ennen sen jälleenlähetystä. Toinen tapa on murtautua tukikohdan järjestelmään ja siellä muuttaa lennätykseen liittyviä tietoja.

Molemmissa tavoissa on hyvät ja huonot puolensa. Satelliittien väliseen kommunikointiin voi olla vaikea kytkeytyä. Toisaalta kun tunnetaan, että signaalin siirtyminen kestää useita sekunteja maan ja satelliitin välillä, voisi olla mahdollista päästä huomaamatta siirtopisteiden väliin.

Ohjauskomentojen lisäksi operaation ja koneen välillä kulkee kuva- ja tiedustelutietoja. Nämäkin signaalit voivat kulkea satelliittien välityksellä samaa reittiä kuin ohjaus. Kumman tahansa datan sekoittaminen voi saada aikaan vahinkoa. Mutta erityisesti ohjausdatan muokkaaminen ja siten koneen toiminnan sekoittaminen väärässä kohtaa saa aikaan tuhoa. Kone voidaan yksinkertaisesti tuhota tai se voidaan saada laukaisemaan asekuormansa väärään kohteeseen.

5. ERILAISIA HYÖKKÄYSTAPOJA JA -TEKNIIKKOJA

5.1 Välimies -hyökkäys

Man in Middle eli välimies -hyökkäys on tavanomainen hyökkäystapa verkossa. Siinä, yksinkertaistettuna, hyökkääjä toimii kahden viestijän välissä ikään kuin releenä tai salakuuntelijana. Tällöin viesti kulkevat hyökkääjän kautta ilman, että varsinaiset osallistujat sitä havaitsevat. Kun hyökkääjä on päässyt väliin, on hyökkääjän mahdollista muokata viestejä jotka kulkevat liikennöitäessä.

Kun ajatellaan sellaista tilannetta, että toisena viestijänä on jokin sensori tai vastaava laite, joka lähettää verkon ylitse dataa muualle vaikkapa analysoitavaksi, voi vastaanottajan olla vaikea tulkita sellaista tilannetta, että dataa on muutettu välissä. Viestijä voi koittaa puolustautua tällaista hyökkäystä vastaan erilaisilla tavoilla. Tällaisia ovat mm. erilaiset autentikointitavat ja vahvat salaukset. Yhtenä keinona on käyttää julkisen avaimen salausta. Välimieshyökkäys toimii kuitenkin useimpia tapoja vastaan, joten puolustautujan on pidettävä huolta, etteivät avaimet tai muu informaatio vuoda muiden tietoon.

5.2 Hakkerointi yritykseen

Eniten julkisuutta saavat hyökkäykset kohdistuvat suoraan yrityksiin. Usein hyökkääjät ovat varastaneet yrityksiltä erilaisia henkilötietoja tai käyttäjätunnus- / salasanapareja. Yrityksien tarkoituksena on pitää tiedot salaisina, käyttäjien eli asiakkaiden ja yrityksen omien etujen vuoksi, mutta murtautujat ovat silti päässeet suurienkin yritysten tietoihin käsiksi.

Hyökkäys yritykseen voi, mikäli suojaukset ovat heikot, tapahtua yksinkertaisestikin saamalla käyttäjätunnuksen ja salasanan käyttöön. Tämä voi tapahtua helposti social engineering -hyökkäyksellä, minkä yksi variaatio on se, että hyökkääjä teeskentelee IT-tukea ja kalastelee tunnukset työntekijältä itselleen.

Todennäköisemmin hyökkäys vaatii aikaa enemmän ja sisältää useita erilaisia tekniikoita, joilla päästään aina pidemmälle sisäverkon puolella. Se saattaa alkaa sillä, että työntekijöille lähetetään sähköpostia, joka sisältää makron tai muun vastaavanlaisen ohjelman, jolla voidaan asentaa haittaohjelma koneelle tai verkkolaitteisiin. Tällä haittaohjelmalla hyökkääjä voi kuunnella ja vakoilla verkkoa ja kerätä tietoa jota tarvitaan seuraavissa vaiheissa. Tämä voi vaatia verkonlaitteiden kuten esimerkiksi reitittimien ja muiden kuuntelua tai niiden konfigurointia.

Tämän jälkeen hyökkääjä voi joutua selvittämään vielä uusia salasanoja ja käyttäjätunnuksia, ennen kuin pääsee tietovarastoon käsiksi. Tämäkin yhteys voi olla salattu sisäisellä VPN -toteutuksella ja voi vaatia kohdassa 5.1 mainittua tekniikkaa. Heikkouksina tässä kohtaa voivat olla väärin tai huonosti konfiguroidut laitteet jotka päästävät hyökkääjän sisälle tai näyttävät liikaa infrastruktuurista. Tai hyökkääjä voi koittaa käyttäjän manipulointia tässäkin vaiheessa hyökkäystä. Joka tapauksessa tästä voidaan havaita, että sisäänpääsyyn voidaan tarvita useita eri tekniikoita. Eri tekniikoiden käyttämisen lisäksi hyökkäys saattaa kestää pitkään. Jotta hyökkääjä saa tietoa verkosta ja sen heikoista kohdista, on hänen tarkkailtava toimintaa verkossa ja mahdollisesti urkittava tai muuten selvitettävä lisää salasanoja. Tämän vuoksi puolustautujan eli tässä tapauksessa yrityksen on tarkkailtava toimintaa sisäverkossaan, ulkoverkonhyökkäysten lisäksi. Se voi olla keino saada hyökkääjä kiinni tai ainakin oppia oman verkon heikkoja kohtia.

5.3 Käyttäjän manipulointi

Social engineering on yleinen englanninkielinen termi käyttäjän manipuloimiselle. Käyttäjän manipulointi on hyökkäystapa, jolla koitetaan saada selville järjestelmään tunkeutumiseen tarvittavia käyttäjätunnuksia ja salasanoja. Tavassa käytetään hyväksi yrityksessä toimivaa henkilöstöä ja koitetaan saada heidät paljastamaan tietoja tai saada asentamaan hyökkääjän ohjelmiston järjestelmään.

Tavassa hyökkääjä yrittää saada jonkinlaisen luottamussuhteen työntekijään, jotta tämä toimisi hyökkääjän haluamalla tavalla. Tätä varten hyökkääjä koittaa selvittää etukäteen yrityksen organisaatiota ja nimiä tai yrityksen liikekumppaneita. Käyttämällä näitä tietoja hyökkääjä voi esittäytyä toisena, luotettavana henkilönä joko yrityksen sisältä tai sitten vaikkapa laskun maksavana osapuolena. Usein käytetty esimerkki on toimia it-tukena, joka on tulossa päivittämään konetta ja tarvitsee tätä varten käyttäjätunnuksen ja salasanan.

Jos hyökkääjä toimii kuin olisi toinen yritys, hän voi koittaa saada asennettua haittaohjelman yrityksen verkkoon. Tämä on mahdollista lähettämällä sähköpostia ja sen mukana liitteen, jossa on haittaohjelma. Tai lähettämällä jonkin muun median missä väittää olevan jotain tarvittavaa tietoa, kuten esimerkiksi sovitun esityksen kalvot tai laskujen liitteen.

6. SUOJAUTUMINEN HYÖKKÄYKSELTÄ

Kuten edellä on jo mainittu datamanipulaatiohyökkäys ei ole helpoin tapa suorittaa kyberhyökkäys. Se vaatii usein järjestelmän hyvää tuntemusta ja mahdollisesti useiden kuukausien tiedustelua kohteessa. Hyökkäyksen suorittaminen saattaa vaatia useita eri tekniikoita ennen kuin kohteeseen edes päästään sisälle. Puolustajan eli datan omistajan suojautumiskeinot vaihtelevat kohteen mukaan ja datan kulkeman reitin mukaan.

6.1 Fyysinen suojautuminen

Jos järjestelmässä on fyysisiä sensoreita, on ne suojattava, jottei hyökkääjä pääse muokkaamaan niiden olosuhteita ja siten dataa jo alkulähteellä. Yleisesti ottaen tämä täyttyy, kun sijoituspaikkaa mietittäessä otetaan huomioon, ettei paikkaan haluta päästää ylimääräisiä henkilöitä. Rakennuksia voidaan suojata eri tavoilla, mutta siihen ei oteta enempää kantaa tässä työssä.

Pelkästään anturin suojaaminen ei välttämättä riitä. Sensoreilla ja antureilla on ajureita ja mahdollisesti jopa omia ohjausohjelmistoja, joiden dataa voidaan myös muuttaa. Kyberiskussa on mahdollista jopa tuhota tai muuten muuntaa käyttökelvottomiksi mittauslaitteita muuttamalla niiden ajureita ja käynnistyssekvenssejä. Koska joissain tapauksissa laitteet saattavat sijaita hajautettuna, etäällä toisistaan ja niitä saattaa olla useita, sensorien vaihtaminen uusiin estää järjestelmän toiminnan vuorokausiksi.

Fyysistä suojausta tarvitaan myös datan varastointipaikassa. Joissain järjestelmissä tiedon käsittelyyn voi olla määritettynä vain yksittäisiä, määrättyjä koneita. Jotta dataa päästäisiin manipuloimaan, on tällaisessa tapauksessa tarpeellista päästä lähelle näitä yksittäisiä laitteita. Tällöin dataan ei muutoinkaan pääse verkon ylitse. Tällaiset järjestelmät ovat harvinaisempia, sillä ne rajoittavat myös käyttäjän toimia, ainakin osittain. Rajoituksia voi olla kuitenkin tehtynä niin, että yhteyden ottavan koneen on oltava jossakin määrätyssä verkossa. Tällöin on hyökkääjän ensin murtauduttava yrityksen verkkoon ja toimittava sieltä käsin.

6.2 Siirronaikana verkossa suojautuminen

Seuraava vaihe datan elinkaaressa on yleensä sen siirtäminen, joko jonnekin tietokantaan tai muistiin tai suoraan toisille käyttäjille. Datan siirrossa hyökkääjän mahdollisuus manipuloida dataa on suorittaa välimieshyökkäys, eli kaapata data matkalla ja muuttaa sitä ennen kuin vastaanottaja saa sen. Tätä vastaan voidaan toimia salaamalla data siirron aikana. Salaukseen on olemassa useita erilaisia keinoja riippuen siitä mitä, data on ja mil-

laista siirtotietä käytetään. Yksi keino on salata itse siirtotie. Käyttämällä erilaisia luotettavia verkkoja voidaan dataa siirtää turvallisemmin kuin salaamattomassa internet yhteydessä. Tällainen tapa voi olla vaikkapa käyttää VPN-yhteyttä kohteiden välillä.

Mikäli dataa siirretään valtioiden lävitse, on mahdollisuuksien mukaan tarkastettava mitä kautta data siirtyy. Joissain tapauksissa on mahdollista reitittää data turvallisempaa reittiä pitkin, vältellen joitain maita. Yksi mahdollisuus, vaikkakin kalliimpi, on vuokrata satelliitti kaistaa käyttöön, mikäli sellaista ei ole valmiiksi kansallisesti käytettävissä.

Kumpikaan näistä keinoista ei poista sitä uhkaa, että dataviestit voidaan kaapata matkalla, mutta riskihallinallisesti tunnettu reitti on parempi vaihtoehto, kuin normaali internetin reititys. Joissain maissa lainsäädäntö mahdollistaa verkkovakoilun tai muutoin on suuri riski sille, että tiedot vuotavat matkalla rikollisten käyttöön.

Datan salaamiseen on olemassa myös valmiita laitteistoratkaisuja. Tällaisia järjestelmiä käytetään ainakin sotilas- ja viranomaisverkkoratkaisuissa. Tällaisilla laitteilla voidaan siirtää STIV ja STIII luokan materiaalia. Joissain tapauksissa on mahdollista siirtää jopa STII dataa laitteiden välillä. Tämän tyyppisessä verkkoratkaisussa sekä vastaanottaja että lähettäjä käyttävät samanlaisia laitteita, joiden välille luodaan VPN-verkko. Salaamiseen voidaan käyttää vahvoja tapoja, kun avaimet voidaan luoda ja tarvittaessa jakaa etukäteen.

6.3 Datavarastossa suojautuminen

Kolmas vaihe on datan tallennus. Tallennettuun dataan pääseminen vaatii hyökkääjältä pääsyn esimerkiksi yrityksen verkkoon ja siellä usein vielä sisäverkon puolelle, jos data on eristetty muusta verkkoinfrastruktuurista. Puolustautumiskeinona onkin pitää tietoturvallisuutta yllä eri keinoilla. Itse data voidaan kryptata ja vielä hajauttaa eri paikkoihin. Pääsynvalvontaan ja eheyden ylläpitämiseen on olemassa omia tekniikoita. Ja yksi tärkeimmistä on huolehtia henkilöstön tietoturvaosaamisesta ja motivaatiosta sen toteuttamiseen. Myöskään erilaisia tapoja tehdä varmuuskopiota ei saa unohtaa.

Koska aina on kuitenkin mahdollista, että hyökkääjä pääsee verkkoon sisälle, on sisäisen verkon valvonta tärkeää, jotta voidaan oppia hyökkäyksistä ja estää niitä tulevaisuudessa. Lisäksi valvonnan tärkeyttä korostaa se, että havaittu mahdollinen outo toiminta verkossa voi paljastaa hyökkääjän, ennen kuin varsinainen isku pääsee tapahtumaan.

7. YHTEENVETO JA ARVIO TILANTEESTA

Vaikka datamanipulaatio tapauksia on vielä vaikea löytää julkisesta tai tieteellisistä lähteistä, voidaan ennustaa, että niiden käyttäminen on lähestymässä. Yleisesti ottaen kyberhyökkäykset ja -häirinnät ovat kasvaneet. Varsinkin Venäjän on väitetty käyttäneen kyberhyökkäyksiä yhtenä osana operaatioissa. Venäjä on tosin kieltänyt kaikki yhteydet ja syytökset hyökkäyksiin. Kyberhyökkäystä on käytetty ainakin Ukrainassa 2014 ja Virossa 2007 [16]. Toinen usein mainittu valtio kyberasioissa on Pohjois-Korea.

Venäjällä ja sen edeltäjällä Neuvostoliitolla uskotaan olevan paras tietotaito yleisesti kybersodan käynnistä. Useita iskuja on teoreettisesti yhdistetty venäläisiin ryhmiin ja samalla kun niitä on analysoitu, on päädytty siihen, että koska iskut vaativat runsaasti resursseja, niillä olisi valtion tuki takana. Työn aikana ei kuitenkaan löytynyt yhtään sellaista hyökkäystä, joka olisi voitu varmasti sitoa venäläisiin. Aihetodisteita on kuitenkin löytynyt. Tällaisia ovat olleet esimerkiksi sellaiset, että hyökkäysten ajat kohdemaissa osuvat Moskovan aikavyöhykkeen virastoaikaan. Ja että hyökkääjien keskusteluista on löydetty venäjän kieltä. Lisäksi kohteet ovat usein olleet sellaisia, joihin venäjällä on intressejä, kuten Ukraina Krimin valtauksen aikaan.

Nykyiset järjestelmät käyttävät yhä enemmän sensoreilla tuotettua dataa ja samalla vanhoja vähemmän tietoa käyttäneitä järjestelmiä päivitetään vastaamaan uusia. Suurella datamäärällä voidaan yhteiskunnassa saada säästöjä aikaiseksi ja tehostaa toimintaa. Sotilasjärjestelmät käyttävät samoin yhä enemmän dataa päätöksenteossa ja järjestelmän laitteet siirtävät dataa keskenään. Esimerkiksi uudet neljännen ja varsinkin viiden polven hävittäjät pyrkivät jakamaan reaaliaikaisesti tietoa uhista keskenään tai antamaan maalitietoa, niin, että operaation koneet voivat iskeä useaan eri maaliin yhtä aikaisesti.

Kyberturvallisuuteen on alettu kiinnittämään yhä enemmän huomiota. Yritykset joutuvat lainsäädännönkin vuoksi huomioimaan yhä paremmin miten suojelevat asiakkaidensa tietoja. Tapaukset joissa krakkerit ovat päässeet isojen yritysten kuten vaikkapa Sonyn tiedostoihin käsiksi ovat nousseet julkisuuteen ja kiinnittäneet huomiota muidenkin kuin uhrien keskuudessa. Valtioiden strategioissa on myös kiinnitetty huomiota kyberpuolustukseen, ja esimerkiksi Yhdysvaltojen puolustukseen kuuluvat sekä kyberpuolustautuminen että -hyökkääminen.

Tätä työtä tehtäessä ei löytynyt yhtään dokumentoitua verkkohyökkäystä, jossa olisi käytetty hyväksi puhtaasti datan manipulointia. Lähin suurimman julkisuuden saanut suoritus on Stuxnet -nimisen haittaohjelman käyttäminen Iranin uraanin rikastuslaitokseen. Ohjelman avulla uudelleen ohjelmoitiin sentrifugien ohjauslogiikka ja näin saatiin moottorit käymään väärällä nopeudella [17].

Datamanipulaatio on mainittu viime vuosina erilaisissa julkaisuissa ja valtioiden uhkakuvien joukossa. Tämä viittaa siihen, että uhka on sekä havaittu, että sitä pidetään todellisena mahdollisuutena. Yhteiskunnalle kriittiset järjestelmät ovat jo kiinni verkossa ja niiden verkkopalvelut ovat arkipäivää monessa maassa. Esimerkiksi Suomessa sähköinen resepti on tullut arkipäiväiseksi tavaksi hallinnoida lääkkeiden liikkumista, määräämistä koko matkan kuluttajalle asti. Mikäli hyökkääjä pääsisi sekoittamaan näissä järjestelmissä käytettävää dataa, sen vaikutukset voisivat olla suuret. Koska joissain tapauksissa ei voida ennustaa, mitä kaikkea voi tapahtua, on täydellisen tapahtumien kulun ennustaminen vaikeaa. Voidaan vain antaa hyviä ennustuksia tai simulaatioita. Joka tapauksessa vaikutukset näkyisivät päivittäisissä toiminnoissa, mikäli hyökkäys onnistuu.

Datamanipulaatio hyökkäyksen voidaan arvioida tapahtuvan lähellä kriisiä tai kun halutaan vaikuttaa maan poliittiseen tilanteeseen. Nämä kaksi liittyvän ainakin osittain toisiinsa, poliittisesti voidaan yrittää vaikuttaa esimerkiksi valtion sotilaalliseen liittoutumiseen tai muutoin suhteisiin toisiin valtioihin. Tällaisia hetkiä ovat useimmat valtiolliset äänestykset. Yleinen ilmapiiri maailmalla on kiristynyt eri kriisien vuoksi ja suuret valtiot ja sotilasliittoutumat pyrkivät pitämään asemansa tai jopa laajentamaan vaikutustaan. On hyvinkin mahdollista, että suomenkin osa liitoutumattomana valtiona houkuttaa toisia valtioita vaikuttamaan sisäpolitiikkaan. Niin kauan, kuin tilanne kuitenkin ei eskaloidu lähelle kriisiä, tuskin datamanipulointia käytetään hyökkäykseen valtiota kohtaan. Tilanteen kiristyessä tällainenkin hyökkäys on mahdollinen. Tämä ei kuitenkaan estä muunlaisia kyberhyökkäyksiä ja vaikuttamisia jatkuvasti maata vastaan.

LÄHTEET

[1] Department of Defence, Cyber strategy, 2015. Referred 19. September 2017. Available: http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf

[2] J.A.Lewis, Compelling Opponents to our will: The role of cyber warfare in Ukraine. Referred 10. November 2017. Available: https://ccdcoe.org/sites/default/files/multimedia/pdf/CyberWarinPerspective_Lewis_04.pdf

[3] EMC digital universe with research and analysis by IDC, The digital universe of opportunities: Rich data and the increasing value of the internet of things. Referred 5. November 2017. Available: http://www.emc.com/leadership/digital-universe/2014iview/index.htm

[4] J.Limnéll, K.Majewski, M.salminen, Kyberturvallisuus, 2014.

[5] S.Wray, Electronic Civil Disobedience and the World Wide Web of Hacktivism: A Mapping of Extra Parliamentarian Direct Action Net Politics, 1998.

[6] Oxford University Press. Referred 23. August 2017. Available: https://en.oxforddictionaries.com/definition/us/terrorist

[7] D. Rassler, Remotely Piloted Innovation: Terrorism, Drones and Supportive Technology, 2016. Referred 5. October 2017. Available: https://ctc.usma.edu/v2/wp-content/uploads/2016/10/Drones-Report.pdf

[8] J.Kosola, T.Solante, Digitaalinen taistelukenttä, 2000

[9] Visual Capitalist, All of the World's Stock Exchanges by Size, February 17 2016. Referred 18. October 2017. Available: http://www.visualcapitalist.com/all-of-the-worlds-stock-exchanges-by-size/

[10] MyPrivateBanking research, Robo-advisors report 2014. Referred 19. September 2017. Available: http://www.myprivatebanking.com/article/robo-advisors-report-2014

[11] Iltasanomat, Pörssin riehuja paljastui: robotti yritti ostaa osakkeita 2,9 miljardilla. Viitattu 29. syyskuuta 2017. Saatavissa http://www.iltasanomat.fi/taloussanomat/porssiuutiset/art-2000001806469.html, Financial Times, maksumuurin takana.

[12] F. Schreier, On Cyberwarfare, DCAF Horizon 2015 working paper No. 7. Referred 19. September 2017. Available: http://www.dcaf.ch/Publications/On-Cyberwarfare

[13] Darpa, FLA project. Referred 11. November 2017. Available**:** http://www.darpa.mil/program/fast-lightweight-autonomy

[14] UNAMA News, UNAMA condemns killing of at least 15 civilians in airstrike, September 2016. Referred 19. September 2017. Available: http://unama.unmissions.org/unama-condemns-killing-least-15-civilians-airstrike

[15] The New York Times, U.S. Admits Airstrike in Syria, Meant to Hit ISIS, Killed Syrian Troops,17. September 2016. Referred 19. September 2017. Available: http://www.nytimes.com/2016/09/18/world/middleeast/us-airstrike-syrian-troops-isis-russia.html

[16] R. Bejtlich, Strategic defence in cyberspace: Beyond tools and tactics, 2015. Referred 19. September 2017. Available: https://ccdcoe.org/sites/default/files/multimedia/pdf/CyberWarinPerspective_Bejtlich_18.pdf

[17] D. Kushner, The Real Story of Stuxnet, 2013. Referred 29. October 2017. Available: http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet